

Qualys VMDR®: Gestión integral, detección y respuesta a vulnerabilidades

Llevamos la solución líder de gestión de vulnerabilidades a un nivel superior

Descubra, evalúe, priorice y corrija las vulnerabilidades críticas en tiempo real y en todo su entorno de TI híbrido global, y con una sola solución.



VMDR con organización integrada



Identifique todos los recursos conocidos y desconocidos en su entorno de TI híbrido global

Saber qué está activo en un entorno de TI híbrido global es fundamental para la seguridad. Detecte automáticamente todos los activos de TI conocidos y desconocidos presentes en el entorno, para obtener un inventario completo y clasificado, enriquecido con detalles como, entre otros muchos, la información de ciclo de vida de los proveedores.



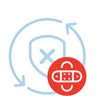
Analice las vulnerabilidades y errores de configuración con precisión Seis Sigma

Detecte automáticamente las vulnerabilidades y los errores de configuración serios según las referencias del CIS, clasificados por activo.



Céntrese rápidamente en lo más urgente

Gracias a la correlación avanzada y al aprendizaje automático, puede priorizar automáticamente las vulnerabilidades con mayor riesgo en los activos más esenciales, reduciendo miles de vulnerabilidades a los cientos que realmente importan.



Proteja sus activos contra las amenazas más críticas

Con solo pulsar un botón puede desplegar el parche más relevante para corregir rápidamente las vulnerabilidades y amenazas en entornos de cualquier tamaño.

Los procesos actuales requieren la participación de varios equipos, con múltiples soluciones individuales, lo que añade una considerable complejidad y tiempo al proceso de aplicación de parches críticos.

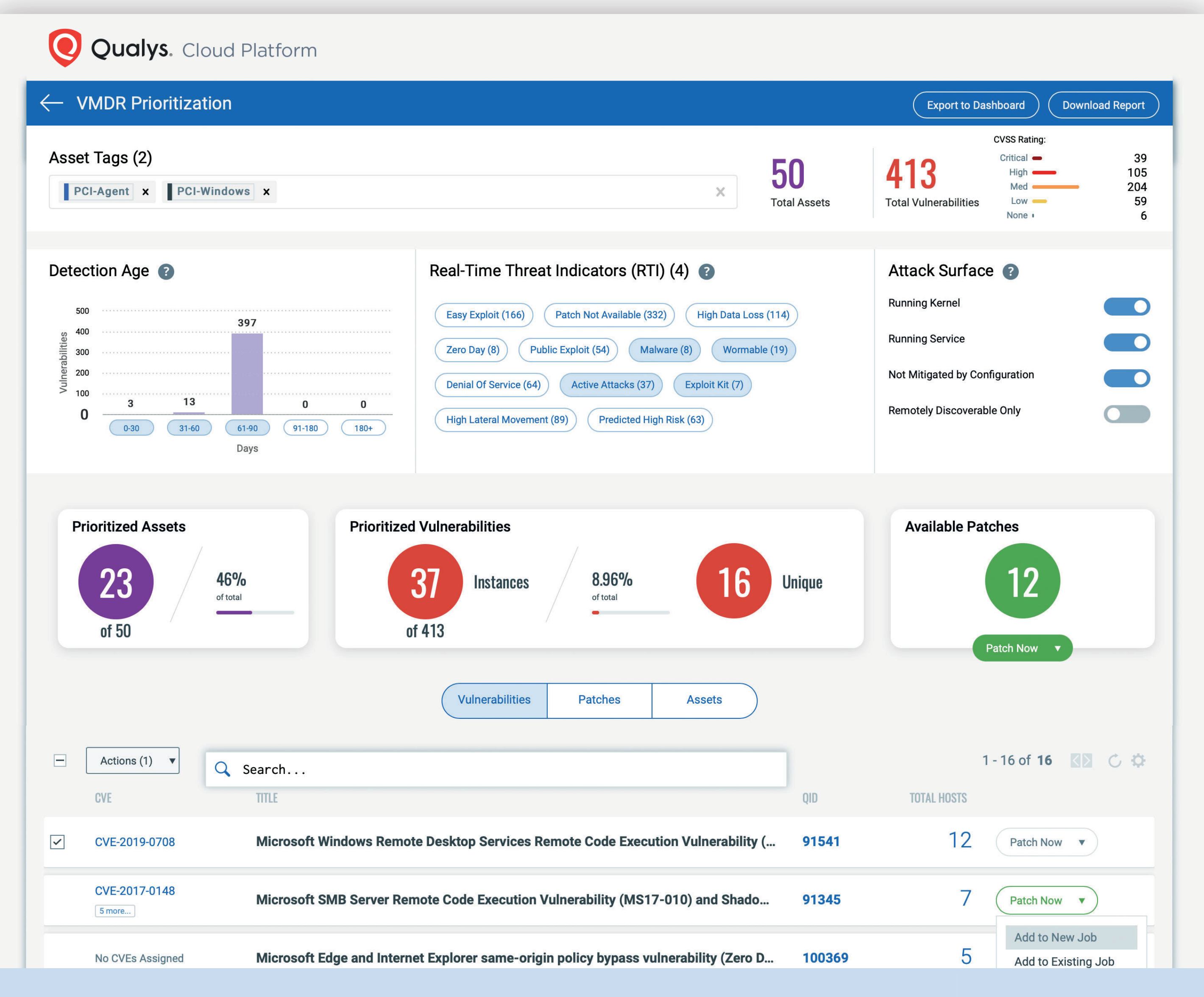
Las soluciones tradicionales para endpoints no interactúan bien, lo que da lugar a problemas de integración, falsos positivos y retrasos. Finalmente, los dispositivos quedan sin identificar, los activos críticos no se clasifican correctamente, las vulnerabilidades no se atienden por prioridades y los parches no se aplican en su totalidad.

Una sola app para el descubrimiento, evaluación, detección y respuesta.

Qualys Cloud Platform, junto a sus agentes en la nube ligeros, sus escaners virtuales y su análisis de red (pasivo) reúnen en una sola app los cuatro elementos esenciales de un programa de gestión de vulnerabilidades eficaz, unificados mediante flujos de trabajo de organización, listos para utilizar. Qualys VMDR® permite a las empresas descubrir automáticamente todos los activos de su entorno, incluidos los no gestionados que aparecen en la red, crear un inventario de todo el hardware y software, y clasificar y etiquetar los activos esenciales. VMDR evalúa continuamente estos activos para descubrir las últimas vulnerabilidades, y aplica la inteligencia sobre amenazas más reciente, con el fin de priorizar de forma activa las vulnerabilidades que se pueden aprovechar. Por último, VMDR detecta automáticamente el último parche para el recurso vulnerable y lo despliega fácilmente para corregir la brecha.

Organización integrada

VMDR, que ofrece todo esto en un solo flujo de trabajo de apps, automatiza el proceso completo y acelera considerablemente la capacidad de la empresa para responder a las amenazas, evitando así posibles ataques.



Ventajas fundamentales



Todo está en la nube

No se necesitan dispositivos que ocupan espacio y recursos. Todo está en la nube y listo para funcionar.



Fácil de desplegar

El despliegue es increíblemente sencillo. Sin límite de escáneres virtuales, puede configurar un analizador y estar listo para que funcione de forma inmediata.



Incluye gestión de vulnerabilidades

VMDR incluye la misma solución de gestión de vulnerabilidades que conoce y en la que confía, así como muchas otras interesantes apps.



Reducción drástica del tiempo y el coste

Con una sola plataforma de la nube, las empresas ahorran bastantes recursos, así como el tiempo que necesitarían para instalar varios agentes y consolas, y para las integraciones.



ADMINISTRACIÓN DE ACTIVOS

Identificación y clasificación de activos automatizadas

Saber qué está activo en un entorno de TI híbrido global es fundamental para la seguridad. VMDR permite a los clientes descubrir y clasificar automáticamente los activos conocidos y no conocidos, identificar continuamente los recursos no gestionados y crear flujos de trabajo automatizados para gestionarlos de manera eficaz.

Una vez que se obtienen los datos, los clientes pueden consultar de forma inmediata los recursos y los atributos para obtener una mejor visibilidad de ellos. hardware, configuración del sistema, aplicaciones, servicios, información de red, etc.



GESTIÓN DE VULNERABILIDADES

Detección de vulnerabilidades y errores de configuración en tiempo real

VMDR permite a los clientes detectar automáticamente las vulnerabilidades y los errores de configuración serios según las referencias del CIS, clasificados por activos. Los errores de configuración pueden generar brechas y provocar el incumplimiento de normativas, creando en los activos vulnerabilidades no incluidas en la lista de vulnerabilidades y exposiciones comunes (CVE, Common Vulnerabilities and Exposures). VMDR identifica continuamente las vulnerabilidades y errores de configuración en la gama más amplia de dispositivos, sistemas operativos y aplicaciones de la industria.



PRIORIZACIÓN DE AMENAZAS

Priorización automática de la corrección

VMDR emplea inteligencia de amenazas en tiempo real y aprendizaje automático para priorizar de forma automática las vulnerabilidades de mayor riesgo en los activos más críticos. Hay indicadores que clasifican las vulnerabilidades como susceptibles de ser aprovechadas, atacadas activamente y con desplazamiento lateral, para destacar las vulnerabilidades actuales que presentan riesgos. Además, los modelos de aprendizaje automático resaltan las que tienen más probabilidad de convertirse en amenazas serias, con varios niveles de prioridad.



PATCH DETECTION

La aplicación de parches y la corrección a su alcance

Correlacione de forma automática vulnerabilidades y parches para hosts específicos, con la consiguiente reducción del tiempo de respuesta y corrección. Busque vulnerabilidades CVE e identifique los últimos parches.

Además, hay tareas recurrentes, automatizadas, basadas en directivas, que mantienen actualizados los sistemas, con una administración proactiva de los parches de seguridad o de cualquier otro tipo. De esta forma se reducen en gran medida las vulnerabilidades que el equipo de operaciones debe controlar, como parte del ciclo de corrección.



Confirmación y repetición

VMDR cierra el bucle y completa el ciclo de vida de administración de vulnerabilidades desde un solo cuadro que incluye paneles y widgets personalizables con identificación de tendencias integrada. Con un precio por recurso y sin necesidad de actualizar software, VMDR reduce drásticamente el coste total de propiedad.

Qualys VMDR® — Véalo usted mismo

Apps y servicios	Funcionalidades	Incluido	Complemento
ADMINISTRACIÓN DE ACTIVOS			
Descubrimiento de Activos	Detecte y cree un inventario de todos los activos conocidos y desconocidos que se conectan a su entorno de TI híbrido global, incluidos los dispositivos y aplicaciones locales, móviles, endpoints, nubes, contenedores, TO e IoT. Incluye sensores de análisis pasivo de Qualys.	○	
Inventariado de Activos Consiga en tiempo real un inventario actualizado de todos los activos de TI.	• **On-premises Device Inventory:** detecte todos los dispositivos y aplicaciones conectadas a la red, incluidos servidores, bases de datos, estaciones de trabajo, enrutadores, impresoras y dispositivos IoT, entre otros. • **Certificate Inventory:** detecte y catalogue todos los certificados TLS/SSL digitales (internos y externos) de cualquier autoridad de certificación. • **Cloud Inventory:** supervise los usuarios, instancias, redes, almacenamiento, bases de datos y sus relaciones para tener un inventario continuo de los recursos y activos en todas las plataformas de nube pública. • **Container Inventory:** descubra y controle la infraestructura de contenedores en todos los entornos. • **Mobile Device Inventory:** detecte y catalogue los dispositivos móviles en toda la empresa, con amplia información sobre el dispositivo, su configuración y las apps instaladas.	○	
Asset Categorization and Normalization	Recopile información detallada, como los detalles de los activos, los servicios en ejecución, el software instalado, etc. Elimine las variaciones de nombres de productos y proveedores, y clasifíquelos por familias de productos en todos los recursos.	○	
Enriched Asset Information	Consiga información avanzada y detallada, como datos de los ciclos de vida del hardware/software (EOL/EOS), de auditorías de licencias de software o de licencias comerciales y de código abierto, etc.		○
CMDB Synchronization	Sincronice bidireccionalmente la información de los recursos entre Qualys y ServiceNow CMDB.		○
GESTIÓN DE VULNERABILIDADES			
Vulnerability Management	Detecte continuamente las vulnerabilidades del software con la base de datos de firmas más completa, en la gama de categorías de recursos más amplia posible. Qualys es el líder del mercado en gestión de vulnerabilidades.	○	
Configuration Assessment	Evalúe, informe y supervise los problemas de configuración, en función de las referencias del Centro para Seguridad en Internet (Center for Internet Security, CIS).	○	
Certificate Assessment	Evalúe sus certificados digitales (internos y externos) y configuraciones TLS en busca de problemas y vulnerabilidades de certificados.		
Otros complementos de evaluación	• **Cloud Security Assessment:** supervise y evalúe continuamente sus recursos de PaaS/IaaS, para detectar errores de configuración y despliegues no habituales. • **Container Security Assessment:** analice las imágenes de contenedores y los contenedores en ejecución en su entorno para descubrir vulnerabilidades muy graves y paquetes no aprobados, y facilitar las iniciativas de corrección. Incluye la posibilidad de analizar en fase de creación, con plug-ins para herramientas CI/CD y registros.		○
DETECCIÓN Y PRIORIZACIÓN DE AMENAZAS			
Continuous Monitoring	Reciba en tiempo real alertas de las irregularidades en la red. Identifique las amenazas y supervise los cambios inesperados que se produzcan en la red antes de que se conviertan en brechas de seguridad.	○	
Threat Protection	Detecte las amenazas más graves y aplique los parches según las prioridades establecidas. Con inteligencia de amenazas en tiempo real y aprendizaje automático, puede controlar totalmente las amenazas en evolución e identificar cuáles corregir primero.	○	
RESPUESTA			
Patch Detection	Correlacione de forma automática vulnerabilidades y parches para hosts específicos, con la consiguiente reducción del tiempo de respuesta y corrección. Busque vulnerabilidades CVE e identifique los últimos parches.	○	
Patch Management a través de otros proveedores	Se integra con sus soluciones de despliegue de parches existentes, como SCCM y otras soluciones de terceros, para reducir significativamente el tiempo necesario para aplicar los parches.		○
Patch Management a través de Qualys Cloud Agents	Agilice el despliegue de parches eliminando la dependencia de soluciones de despliegue de terceros mediante Qualys Cloud Agents.		○
Container Runtime Protection	Proteja, asegure y supervise los contenedores en entornos tradicionales de contenedores basados en hosts y contenedores como servicio, con la aplicación de directivas de comportamiento específicas. (Disponible en el 2.º y 3.er trimestre de 2020)		○
Mobile Device Management	Supervise, gestione y proteja de forma remota sus dispositivos móviles. (Beta disponible el 2.º trim. de 2020)		○
Renovación del certificado	Renueve los certificados que caducan directamente en Qualys (disponible en el 2.º trimestre de 2020)		
VMDR incluye, SIN LÍMITE: Qualys Virtual Passive Scanning Sensors (para descubrimiento), Qualys Virtual Scanners, Qualys Cloud Agents, Qualys Container Sensors y Qualys Virtual Cloud Agent Gateway Sensors, para la optimización del ancho de banda.		○	